A Discussion Of Information Warfare From A Taiwanese Perspective

By Tschai Hui-chen, Major General, Republic of China Armed Forces

Editorial Abstract: Major General Tschai Hui-chen outlines the characteristics of Taiwan's IW concepts, discussing control of an enemy, mobilization mechanisms, and "using energy to release changes in patterns." She addresses important aspects of China's IW capability, such as the concept of "network psychological warfare," in which Chinese "Internet opinion personnel" impersonate regular users in Internet discussion forums.

Introduction

With the advent of the information-based society there are also new forms of criminal activity, featured by endless security incidents such as hacker attacks on networks. This has an enormous impact on governments, economies, militaries, and psychologies in countries all over the world. The use of information technology in military operations and weapon systems has fundamentally changed traditional ways of thinking about military operations. The concepts and related theories of information warfare have become the mainstream in modern thinking about war. Even more so, terrorists make use of platforms afforded them by networks as tools to attain their objectives. For example, B.W. Dearstyne holds that management of information and intelligence in American society provided the 9/11 attackers with their opportunity, due to how easily they acquired information.

This article looks at the development of information warfare (IW) and information security in Taiwan from a Taiwanese perspective, and considers the potential risks and challenges presented by the Internet. It explains how Taiwan can make use of its strengths in the area of information technology, to make an effective contribution and put forth its efforts in today's fight against information terror and extremism.

The Development of Information Warfare in Taiwan

Taiwan's Ministry of Defense established the Strategic Commission for Information Operations in 1999, opening the door to the development of information warfare. Developments in theoretical research and principles subsequently led to the establishment of dedicated units in these areas.

The results of a Research, Development, and Evaluation Commission survey under the Executive Yuan showed that Internet access in Taiwan increased from 70.6% in 2005 to 74.5% in 2006. This indicates information networks in Taiwan are quite widespread. Symantec's Internet Security Threat Report noted the United States experienced the most activity involving malicious programs in the first half of 2007, while Taiwan was ranked eighth. This shows network attacks have increased as networks themselves have become more universal. Attacks on military facilities will incur the greatest impact, which is why development of information security and information warfare is a required strategy to prevent and control malicious attacks.

Definition of Information Warfare

The development of information warfare in Taiwan can be defined both broadly and narrowly. The broad definition involves conflict and war between two antagonists, to gain a strategic advantage (or the advantage in war) using the means of information technology in the areas of politics, economics, society, science, technology, and military affairs. The narrower definition includes the following:

(1) Use of information technology to conduct explorations and surveys on the opposition, as well as countermeasures involved in said actions, such as reconnaissance, interference, and disruption;

(2) Combat actions undertaken against the reconnaissance, command, control, communications, information analysis, camouflage, deception, attacks, and destruction activities of the enemy;

(3) Preventative measures undertaken against the interference, disruption, and countermeasures perpetrated by the enemy.

These illustrate that the scope of information warfare includes any measure taken against an enemy, such as information intervention, interference, disruption, breakdown, countermeasures, and counter-countermeasures.

Characteristics of Information Warfare

By contrast with traditional warfare, one could say that information warfare results in victory without firing a shot, or gaining a decisive victory from many miles away. The various IW characteristics illustrate this:

(1) Attackers on an information battlefield do not require enormous financial means, and do not need to purchase expensive equipment. Instead, they need only be able to use and operate the tools of attack (such as Trojan Horses) to be victorious in information warfare—or even inflict severe injury on the opponent;

(2) Traditional distinctions between war and peace, military and non-military, nation and place, and even attacking and defending have become obscured;

(3) The distinction between peacetime and wartime is fading away. Any security leak in an information system can attract an information warfare attack;

(4) Information warfare presents great difficulties for command and control. Battle rhythms move fast, which is why decision-making models

and systems are adjusting to meet these challenges. From the decision-making perspective, the objective in information warfare is to influence (and even break down) the enemy's decision-making mechanism.

Offensive Information Warfare

From an organization and implementation perspective, recent regional conflict actions describe the main features of information warfare at the strategic, campaign, and tactical level. Type actions include:

(1) Long-term and frequent full-scale wars;

(2) Tangible and intangible battle lines in total wars;

(3) Special wars which determine victory or defeat in open conflicts.

Weapons of attack primarily include various types of software viruses, and logic bombs to disrupt computer and communication systems.

Defensive Information Warfare

Defensive information warfare primarily means information security. Security of information and information systems can be measured through the following properties:

(1) Information confidentiality: Ensuring that information is not leaked to unauthorized persons;

(2) Information integrity: Preventing unauthorized tampering, and ensuring that true information is transmitted to its destination without being distorted;

(3) Information authenticity: Information sources can be correctly identified;

(4) Information availability: Ensuring information and information systems are accessed by authorized users and authorized management, which prevents denial of service caused by computer viruses or human actions;

(5) Non-repudiation: Ensuring people performing information activities cannot deny their own activities.

Military Deception

Military deception involves the utilization of electronic interference, camouflage, deception, and network piracy, then integrating them with military force and firepower to create an enormous information attack momentum or threat. Or, it may involve rendering the enemy unwilling to act rashly by "feinting to the east but attacking from the west," giving the appearance of formidability, making secret war plans, tricking the enemy into action, or threatening the enemy psychologically. Potential deception measures include:

(1) A balanced information flow;

(2) Spreading false information in order to deceive the enemy's intelligence, reconnaissance and information gathering;

(3) Making use of terrain and geographical features to secretly allocate and camouflage installations and facilities;

(4) Creating false targets, signals, platforms, and positions, as needed or according to plan.

Taiwan, Republic of China (Wikimedia)

Taiwan's Developmental Policies for Information Warfare

On the basis of the "Total Civilian Defense" policy of 2002, the military buildup transformed from a passive to a proactive policy, and the strategic vision known as "a resolute deterrence and an effective defense" changed to an aggressive defense vision of "an effective deterrence and a resolute defense." The overall military communications and electronic information plan in the Republic of China involves the objectives of attaining information superiority, solidifying national defense, controlling the enemy, and seizing the initiative based on the strategic guidance of and demand for joint operations for "an effective deterrence and a resolute defense." At the same time, the government promotes the following policies based on the concept of the integration of peacetime and wartime activities:

(1) Building up an information infrastructure for national defense: The primary task is coordinating various promotional programs for building a national information infrastructure, and exerting every effort toward advancing the information infrastructure buildup for national defense. This involves constructing networks connected to the military information transmission trunk, as a means of providing the transmission and exchange of systems information for war intelligence, command, management, human resources, logistics, and finances; and utilizing various networks and local linkups to exchange information.

(2) Establishing operational capabilities based on information superiority: The objective for information warfare in Taiwan is to protect communications for national defense, information systems, and network security. Guided by priority protection and quickly seizing the initiative, Taiwan will adopt all measures of proactive surveillance and reconnaissance and aggressive protection. We will set up protective communications and information capabilities, which will include early warnings, and adjustments according to changing circumstances.

(3) Effectively integrating communications and information networks: In order to meet the demands of future operational tasks, Taiwan will continue to advance the formation of new generation military communications,

information installations, and equipment, along with the overall planning for and integration of communications resources. We will strengthen integration of the operational environment and platforms for communications and information systems. We will construct a joint operations communications system featuring operational compatibility, with the goal of integrating the different military services and joint warfare networks.

(4) Integrating command, control, communications, information, intelligence, surveillance, and reconnaissance systems: As a means of exploiting Taiwan's new generation of fighting power, the nation is concentrating its efforts on construction of an integrated command, control, communications, information, intelligence, surveillance, and reconnaissance system (C4ISR) to link up the joint operations command and control system with weapons platforms. This will enable prompt synchronized exchange of intelligence and information, improve transparency on the battlefield, eliminate the fog of battle, and initiate the buildup of an instantaneous command and control system which can see, hear, and command. This will be a key goal in establishing information superiority in Taiwan and exploiting the nation's information operations capabilities.

(5) Strengthening electronic warfare operations capabilities: In response to future forms of war and the demand for joint operations, Taiwan is putting all of its efforts into reorganization of defensive equipment for electronic warfare. This includes EW combat capabilities, and frequency spectrum management capabilities for both attacking and defending. We must ensure communications discipline and information security protection as a means of enhancing IO combat power.

Guided by these policies, Taiwan will formulate a three-phase developmental plan for information warfare:

(1) First phase: Establish information research organizations and formulate information warfare educational programs. Plan for the buildup of infrastructure for national defense information. Draw up an outline for information warfare.

(2) Second phase: Build up the infrastructure for national defense information and set up an information strategy research center. Integrate resources at the Chung-shan Institute of Science and Technology to research and develop IW technology. Establish an information warfare research unit at National Defense University and set up an information warfare team and command mechanism.

(3) Third phase: Integrate national resources and finish planning for a mobilization mechanism for information warfare. Concentrate information combat power in the military, and support Taiwan-Penghu defensive operations.

The Evolution of an Information Security Strategy in Taiwan

The Executive Yuan [Republic of China executive branch of government] passed the "National Communication and Information Infrastructure Security Mechanism Plan" in January 2001, and established the National Information and Communication Security Task Force (organizational structure given in Figure 1) as a means of aggressively promoting its national information and communications security policies. The group integrates, coordinates, and effectively utilizes the resources of relevant government agencies, in order to accelerate construction of a national security environment and enhance national competitiveness. In addition, these act establish of an information security protection system, provide for inspection of information security contingency capabilities, and the establish a sound developmental environment for information security. The following summary of current information and communications security actions shows how Taiwan is meeting swift-growing trends in science and technology, as well as dealing with developments on both sides of the Taiwan Strait:

1. Promotion of Awareness of Information and Communications Security, Personnel Training, and International Collaboration. Considering international developments and the current domestic environment, promoting information and communications security awareness (and training personnel) joins international collaboration as a necessary future trend. Strengthening participation in international information security activities will help establish regional and global joint defense mechanisms for information security. Working together to attack network crime and aggressively promoting global information security are especially important.

2. Aggressive Promotion of Information and Communications Security Operations for Key National Infrastructure Institutions. Electronic information and technologies afford us the ability to closely link critical internal infrastructure and administration in the Taiwanese government, including security, financial services, energy facilities, the water supply, telecommunications, postal services, transportation, shipping, medical care, and other important national economic and security activities. This exposes more potential weak points, presenting opportunities to those with malicious intent, or those not be averse to attacking Taiwan with armed force. As such, Taiwan must build on the foundation of existing national information and communications security efforts by strengthening critical national infrastructure and institutions. This will include the establishment of information security notifications and contingency mechanisms, information sharing mechanisms, establishing information security technology and inspection service teams, providing technology and inspection services, managing the critical infrastructure buildup of information security systems, promoting widespread security education and training, and promoting information security management system verification. This will be effective in providing the best security safeguards during the build-up of infrastructure

3. Widespread Application of Wireless Networking and the Flourishing Development of ISP Providers. Wireless communications have developed rapidly ever since the discovery of electromagnetic waves at the end of the nineteenth century. Wireless communications are an inescapable part

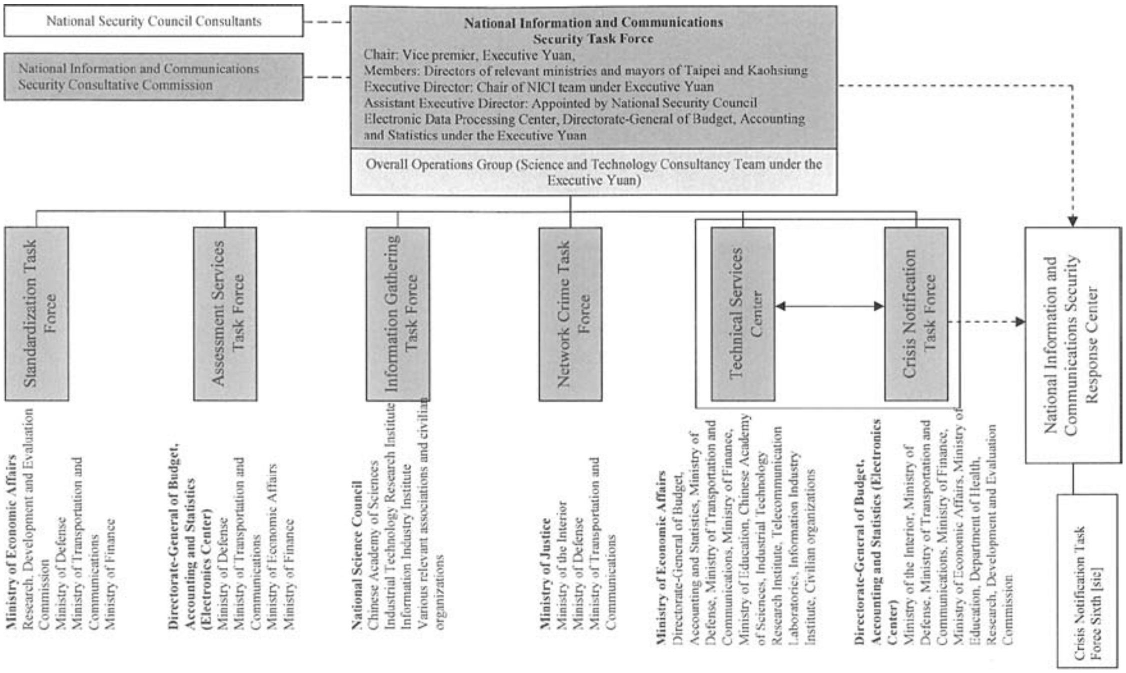
National Security Council Consultants
National Information and Communications Security Consultative Commission
National Information and Communications Security Task Force
Chair: Vice premier, Executive Yuan,
Members: Directors of relevant ministries and mayors of Taipei and Kaohsiung
Executive Director: Chair of NICI team under Executive Yuan
Assistant Executive Director: Appointed by National Security Council
Electronic Data Processing Center, Directorate-General of Budget, Accounting and Statistics under the Executive Yuan
Overall Operations Group (Science and Technology Consultancy Team under the Executive Yuan)
Standardization Task Force
Assessment Services Task Force
Information Gathering Task Force
Network Crime Task Force
Technical Services Center
Crisis Notification Task Force
National Information and Communications Security Response Center
Ministry of Economic Affairs
Research, Development and Evaluation Commission
Ministry of Defense
Ministry of Transportation and Communications
Ministry of Finance
Directorate-General of Budget, Accounting and Statistics (Electronics Center)
Ministry of Defense
Ministry of Transportation and Communications
Ministry of Economic Affairs
Ministry of Finance
National Science Council
Chinese Academy of Sciences
Industrial Technology Research Institute
Information Industry Institute
Various relevant associations and civilian organizations
Ministry of Justice
Ministry of the Interior
Ministry of Defense
Ministry of Transportation and Communications
Ministry of Economic Affairs
Directorate-General of Budget, Accounting and Statistics, Ministry of Defense, Ministry of Transportation and Communications, Ministry of Finance, Ministry of Education, Chinese Academy of Sciences, Industrial Technology Research Institute, Telecommunication Laboratories, Information Industry Institute, Civilian organizations
Directorate-General of Budget, Accounting and Statistics (Electronics Center)
Ministry of the Interior, Ministry of Defense, Ministry of Transportation and Communications, Ministry of Finance, Ministry of Economic Affairs, Ministry of Education, Department of Health, Research, Development and Evaluation Commission
Crisis Notification Task Force Sixth [sic]

Figure 1. Structural organization of the National Information and Communications Security Task Force (National Information Security and Communications Task Force, Taiwan)

of life, whether in military or commercial applications, or in one's daily life. While enjoying the benefits that wireless technology brings, we cannot ignore associated security issues. In addition to technical administration, we must promote administrative measures, such as formulating wireless network security policies thorough examinations of equipment, security contingencies, and investigations. This will reduce risks to an acceptable level, as a means of striking a balance between enjoying the benefits of technology and maintaining concern for security. Preventing and controlling criminal activity in networks requires that we enact laws and regulations, regulate ISP providers, and keep historical audits and usage information as necessary. But it also means strengthening self-defense and accommodating the investigations into equipment, technology, and personnel performed by law enforcement agencies.

4. Contingencies for Potential Threats of Hacker Attacks and Information War. While enjoying the benefits of the Internet we are also exposing ourselves to threats. Interested people can pilfer our personal information by means of penetration or monitoring. Hacking incidents are increasing as Internet access becomes commonplace almost everywhere. Increasingly, average users are placing higher demands on the prevention of illegal attacks. This is why Taiwan emphasizes use of human resources to advance various security means, in order to achieve its comprehensive anti-hacking objectives.

5. Establishing Sound Regulations for Information Security. Taiwan's laws and regulations for information and communications security can be traced back to April 20, 1987. The Executive Yuan enacted a directive entitled "Standards for Maintaining Computer Equipment Security and Confidentiality of Information for Agencies under the Executive Yuan" (Tai Ching Tzu No. 7501). The Internet was not yet prevalent, so the directive primarily regulated computer equipment security, information confidentiality, and the control of information operations. It was superseded by the "Regulations on Information Security for the Executive Yuan and its Subordinate Agencies" on September 15, 1999.

6. Primary Developmental Trends in the Regulation of Information Security.

(1) Enact technical standards for information and communications security;

(2) Enact regulations and reference guides for operations related to information and communications security performed by various government agencies;

(3) Plan and build test technology for information and communications security;

(4) Plan and build authentication procedures for information and communications security.

Threats and Challenges

In a speech to high-ranking People's Liberation Army cadres, Chinese Communist Party Chairman Hu Jintao stressed that the PLA must strengthen its information warfare capabilities, to ensure it will be able to win regional wars featuring high technology, in any potential conflicts. In response to the PRC's advancents in capabilities, Taiwan's *2007 National Defense Report* noted the Chinese Communists' potential to attack Taiwan in the future will include multidimensional modes: complete information and electronic paralysis; long-range precision strikes; rapid warfare; in addition to carrying out potential measures such as deterrence, paralysis, and strategic warfare.

Chinese Communist research into information warfare began with the experiences of the United States in the First Gulf War. The Chinese Communists' understanding of information warfare is mainly that it is a new form of war, and that it uses energy to release changes in patterns. In particular, the Chinese Communists believe future military operational space will be "five-dimensional," and that cyber warfare and space warfare have become the new frontiers for competition between countries. So-called "five-dimensional" operations refer the realms of "land, sea, air, space, and electromagnetics," along with the idea of taking war from the conceptual level to the level of reality.

Widespread utilization of information systems means that information and network security have become ever more critical national security issues. As such, information and network systems and facilities are now key infrastructure. In addition to general sorts of commercial, hacker, and criminal attacks, information security faces organized network attacks perpetrated by China. These have become a daily occurrence, and are a major threat to information security:

1. General Information Security Threats. Information security incidents such as hacking websites, tampering with Web pages, and stealing information are frequent events. Types and means of threats include:

(1) Spreading malicious code: This includes viruses and Trojan horses, as a means of sabotaging computer operations and stealing information.

(2) Unauthorized access: Account passwords are stolen and system security leaks are exploited or passwords are cracked to infiltrate computer hosts in order to delete, alter, or steal information.

(3) Setting up fake websites for organizations or fake network services. "Phishing" refers to obtaining users' private information such as account numbers, passwords, and identification files by deception.

2. Threats from Strategic Information Warfare.

(1) Information warfare is not limited to attacks on information and network systems. Information warfare achieved importance as early as the 1990-91 Gulf War. American think tanks proposed the idea of "strategic information warfare," using of the news media and psychological propaganda in addition to attacks on information and network systems themselves. Perception management is utilized to influence the masses' political perception of their governments. In other words, it refers to both information content and information conflicts being broadcast.

(2) Based on its views of "asymmetric war," China has for a long time aggressively been putting resources into IW research and development. In addition to emphasizing attacks on information networks, China is combining public opinion, psychological, and legal warfare in an organized and systematic fashion, stressing its so-called "Three Warfares." The PRC has unleashed strategic information and message attacks, and is attempting to break down Taiwan's defensive strengths by misleading the masses, confusing our perception of who is an enemy and who is a friend, and weakening the morale of the people.

3. Security Threat Posed by China's Emphasis on Information Warfare. China's utilization of information warfare is extensive in both attacking and defending. When it comes to defense, China has assembled a dedicated team of "network police" to perform surveillance of the activities of Web surfers, and has set up its "Golden Shield Project" (dubbed the "Great Firewall") for comprehensive surveillance and control of the content and flow of network messages. The Information Industry Ministry has a new regulation requiring website owners register with the government, or their websites will be shut down. Even foreign companies must submit to network surveillance, otherwise China prohibits anyone from investing in them. In terms of attacks, Communist China has used following means against Taiwan:

(1) Organizing a large-scale network force: The explosive growth in Internet use in China has not only attracted investment from information industries throughout the world; China has taken this opportunity to develop its information warfare capabilities. It has established what it calls a "Cyber Army," which gathers intelligence on foreign governments and enterprises. Further, it becomes an attacking force when necessary, paralyzing opponents' computer networks. In fact, many western countries, along with Japan and Taiwan, have been subject to frequent network attacks. While some of them have been perpetrated by hackers working independently, the majority originated in specific domains within Chinese territory, and were clearly organized actions.

(2) Network psychological warfare: One could say China is the only country engaging in large-scale Internet and public opinion warfare. In addition to the defensive and control measures noted above, China has been even more aggressive in organizing professional "Internet opinion personnel." These number upwards of fifty-thousand people whose main task involves impersonating regular users in Internet discussion forums. When opinions arise which are unfavorable toward the Chinese government, they defend the government views, and even launch counterattacks. Their primary goal is to manipulate public opinion. In addition, China has incorporated cell phone communications within the sphere of control, so that all text messages are monitored.

Opportunities and Turning Points in the Fight against Information Terrorism

Criminal activity and attacks in the information realm are increasing, and they are problems of great concern. In particular, terrorists have moved from traditional ways of thinking to using the broad reach of network platforms to achieve their ideals and objectives. Today's democratic nations need to consider and pay particular attention to this issue. There is a critical need for policies to meet this new and unprecedented crisis. Before we think about how to approach information

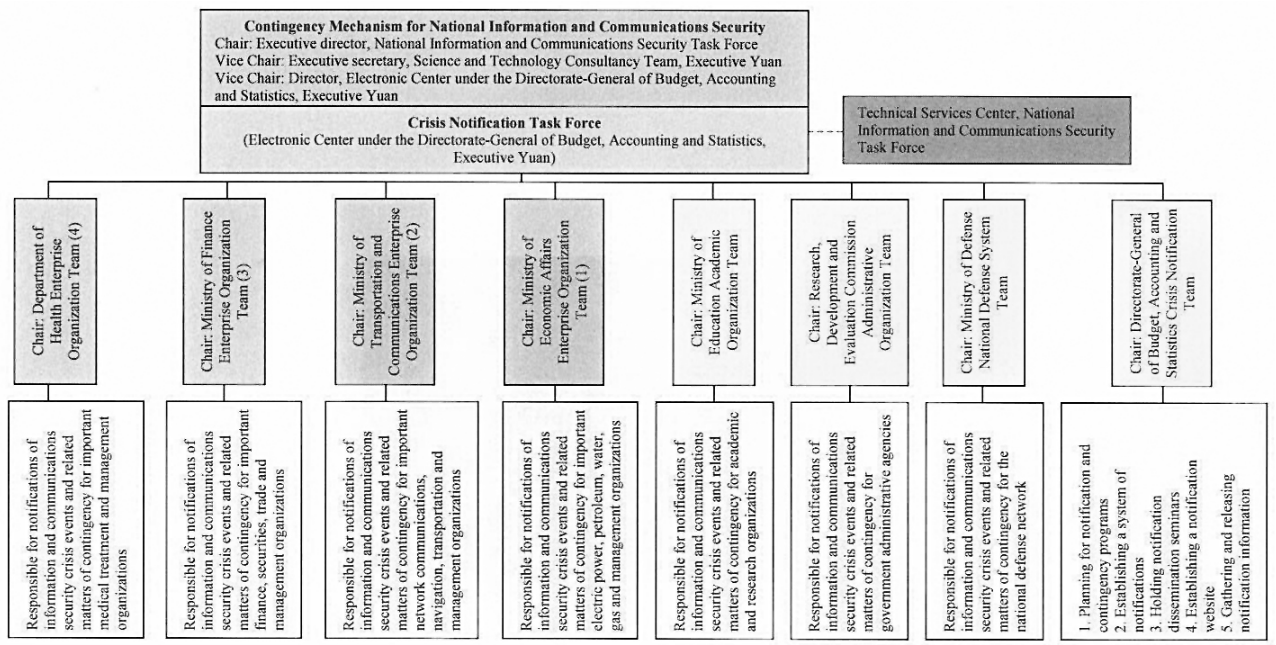
Contingency Mechanism for National Information and Communications Security
Chair: Executive director, National Information and Communications Security Task Force
Vice Chair: Executive secretary, Science and Technology Consultancy Team, Executive Yuan
Vice Chair: Director, Electronic Center under the Directorate-General of Budget, Accounting and Statistics, Executive Yuan
Crisis Notification Task Force
(Electronic Center under the Directorate-General of Budget, Accounting and Statistics, Executive Yuan)
Technical Services Center, National Information and Communications Security Task Force
Chair: Department of Health Enterprise Organization Team (4)
Chair: Ministry of Finance Enterprise Organization Team (3)
Chair: Ministry of Transportation and Communications Enterprise Organization Team (2)
Chair: Ministry of Economic Affairs Enterprise Organization Team (1)
Chair: Ministry of Education Academic Organization Team
Chair: Research, Development and Evaluation Commission Administrative Organization Team
Chair: Ministry of Defense National Defense System Team
Chair: Directorate-General of Budget, Accounting and Statistics Crisis Notification Team
Responsible for notifications of information and communications security crisis events and related matters of contingency for important medical treatment and management organizations
Responsible for notifications of information and communications security crisis events and related matters of contingency for important finance, securities, trade and management organizations
Responsible for notifications of information and communications security crisis events and related matters of contingency for important network communications, navigation, transportation and management organizations
Responsible for notifications of information and communications security crisis events and related matters of contingency for important electric power, petroleum, water, gas and management organizations
Responsible for notifications of information and communications security crisis events and related matters of contingency for academic and research organizations
Responsible for notifications of information and communications security crisis events and related matters of contingency for government administrative agencies
Responsible for notifications of information and communications security crisis events and related matters of contingency for the national defense network
1. Planning for notification and contingency programs
2. Establishing a system of notifications
3. Holding notification dissemination seminars
4. Establishing a notification website
5. Gathering and releasing notification information

Figure 2. Structural organization of the National Information and Communications Security Contingency Center (National Information and Communication Secuirity Task Force, Taiwan)

terrorism, we need to understand how terrorists make use of information to achieve their goals:

7. Methods of Information Warfare Used by Terrorists. Only by understanding the IW methods available to terrorists, and knowing the e nemy as you know yourself, can we achieve victory. Terrorist tactics are mostly similar to those used by the average computer criminal, but there are notable differences:

(1) Most computer criminals will attempt to erase their tracks after committing crimes, so that they can escape scot-free. By contrast, if the terrorist's objective is shock effect, he will typically attempt to create as large a public impact as possible when he paralyzes a system;

(2) Most computer criminals are in it for their own pecuniary benefit. Alternately, terrorist attackers typically consider themselves to be righteous, and very few act for pecuniary benefit for fear of getting involved in disputes. Nevertheless, terrorists often make use of networks to launder money;

(3) Unless they are engaged in retribution, very few computer criminals aim to destroy computers and other support equipment. Information terrorists may attack and destroy physical equipment.

8. Methods of Information Terror Attacks. Having reviewed the differing modes of attack, one can imagine that the terrorists' methods of attack would include the following:

(1) Stealing confidential information: Terrorists make use of network attacks, social engineering, and human contact to steal important classified or sensitive information;

(2) Paralyzing systems: Terrorists make use of malicious code such as viruses, Trojan horses, and worms. They also paralyze systems, make information disappear, and engage in denial of service attacks;

(3) Physical destruction: Terrorists engage in the sabotage, especially government information systems (military, economic, defense, diplomatic, etc.) as a means of paralyzing government operations.

9. The Contribution Taiwan Can Make in the Fight Against Terror. Once we understand terrorist information warfare tactics and methods, what kind of contribution can Taiwan make in the war against terror using our existing information technology?

(1) Taiwan's legal efforts in the War Against Terror have produced its Anti-Terror Activities Act;

(2) Taiwan has formed anti-terror organizational structure that combines various national security systems and the Executive Yuan;

(3) Taiwan's potential contributions include:

1. Taiwan has never had any terrorist activity nor the conditions for its presence. However, terrorism as a form of organized crime crosses borders to obtain funding. These criminal activities include smuggling drugs, human trafficking, money laundering, and other inappropriate financial operations. These are important security issues for Taiwan. With ample evidence of terrorist crimes, plus clues for tracking their activities, we could pursue these criminals. Taiwan could also establish cooperative mechanisms, and strengthen existing ones, to help other countries prevent terrorist activities.

2. In the future, regional terrorist groups might wish to use Taiwan as a gateway for their support or planning activities, in order to strengthen their disruptive activities in other Asian countries. Taiwan can effectively prevent terrorist elements from entering

and leaving the country by strengthening its overall security control capabilities. Rigorous surveillance actions can show evidence of terrorist activities, and provide early warning.

10. Opportunities are Turning Points. Taiwan ranked sixth among 64 countries surveyed in the "IT Industry Competitiveness Index" released by the Economist Intelligence Unit in 2007. However, Taiwan is first in the area of IT labor productivity and third in the area of environment for research. This illustrates Taiwan's notable information and network technology strengths.

In his book *The World is Flat*, Thomas L. Friedman describes *"the rise of Netscape and the dotcom boom that led to a trillion dollar investment in fiber optic cable; the emergence of common software platforms and open source code software enabling global collaboration; and the rise of outsourcing, offshoring, supply chain planning, and insourcing (also known as insourcing where internal business is taken on)."* Friedman held that these flatteners converged in 2000 and *"created a flat world: a global, web-enabled platform for multiple forms of sharing knowledge and work, irrespective of time, distance, geography, and, increasingly, language."* This is why we believe that even though the Internet world is full of dangers, it contains opportunities and turning points.

(1) Opportunities

Even though every corner of the world is different, due to geography, culture, religion, and economics, the rise of the Internet has shortened the gaps between people. Every second that the clock ticks, various types of information speed along fiber-optical cables and via microwaves to every corner of the Earth. The concept of the global village has taken shape, so every country in this new century has an opportunity for collaboration. Taiwan holds an important strategic position which is pivotal in the Asia-Pacific region. We have already constructed a Contingency Mechanism for National Information and Communications Security, allowing our nation to share information, and collaborate with any country in the area of network security.

(2) Turning Points

In the future, the world will be highly information-based. Rapid and instant information will be the key to survival. "The Earth is round, but the world has been flattened by the information highway." Taiwan is situated within this torrent of information. Based on its efforts and guided by the right policies it will emerge as a major information power.

1. We have excellent and indispensable technical human resources—we were the first to discover the method behind the zero-day attack.

2. We are open and willing to share our practical experience with friends.

3. We never fail to do the right thing.

Taiwan can make use of the incredible reach of the Internet to make its contributions in the elimination of global extremism. The distance between countries has been shortened by information networks, and utilization of the Internet to eliminate terrorism will be the turning point in the struggle for world peace.

Conclusion

World trends are even harder to fathom now that we have entered the era of information networks. Their gradual application throughout the world brings a new kind of international influence. At the end of 1999, a United Nations appeal recommended the Internet be seen as an effective tool for global justice, and as the communal wealth of humanity. However, in the "New Economy" where information technology and knowledge innovation are used to create value, is still the privilege of wealthy countries. Most developing nations are still "information poor, left behind by the "digital divide," and may be cast further to the margins of the global economy. The War on Terror is a struggle which never ceases, and nobody knows when the next disaster is going to happen. As such, we will rely upon government policy, buildup of network infrastructure, and improvements to information security to minimize damage—or even prevent terrorist attacks from happening again.

Future wars will tend to be multifaceted. Rapid and instant information will be the key to overall victory or defeat. Information warfare is a new pattern of conflict which has developed against the backdrop of this trend. Recent terrorist incidents have occurred in major cities in several countries, turning terrorism into the major focus of attention, and making it very apparent that our anti-terror actions cannot be delayed.